ECS 152A: Computer Networks Project 1A

Monitoring Live Network Traffic
Professor Zubair Shafiq

Krystal Chau, SID: 920918540 Jacob Feenstra, SID: 921423591

November 3, 2023

1 File Submissions

The following files were submitted along with this `proj1a` PDF.

1. `proj1a-1.pcap`
2. `proj1a-2.pcap`
3. `proj1a-3.pcap`
4. `proj1a-4.pcap`
5. `proj1a-5.pcap`
6. `proj1a-1.py`
7. `proj1a-2.py`
8. `proj1a-3.py`
9. `proj1a-4.py`
10. `proj1a-5.py`

2 Questions

1. List the different application layer protocols and their counts for each activity. In your report, specify how you figured the protocol for each activity

Exercise 1: Used network layer protocol (ICMP - 40)

Exercise 2:	HTTP	30
	HTTPS	109

Exercise 3:	HTTP	4
	HTTPS	31

Exercise 4: FTP - 3

Exercise 5: SSH - 15

Each protocol, particularly on the application layer, has a designated port for its packet transmission. For example, HTTP makes use of port 80, and HTTPS makes use of port 443. We were able to distinguish all relevant application layer protocols by comparing the source/destination port listed for the packet, from Wireshark. FTP uses port 21, and SSH uses port 22. This functions as a unique identifier for the packet's application-layer protocol.

2. How many HTTP and HTTPS packets did you record while performing activities 2 and 3?

Exercise 2:	HTTP	30
	HTTPS	109

Exercise 3:	HTTP	4
	HTTPS	31

3. List the destination IP address used in each activity along with their timestamps. The destination IP address should be in the IPv4 format like x.x.x.x (e.g., “192.168.1.1”, “8.8.8.8”, “10.0.1.150”, etc.).

   Since it mentions destination IP only, we list those timestamps belonging only to outbound packets. We do not include packets being returned to the user’s end-system, since it would then be the source IP. Requests only, and not responses.

Exercise 1:	Destination IP -	142.250.189.206
	Timestamps -	2023-10-31 00:22:41.715105+00:00
		2023-10-31 00:22:42.724427+00:00
		2023-10-31 00:22:43.732492+00:00
		2023-10-31 00:22:44.743817+00:00
		2023-10-31 00:22:49.625413+00:00
		2023-10-31 00:22:50.644027+00:00
		2023-10-31 00:22:51.649177+00:00
		2023-10-31 00:22:52.656517+00:00
		2023-10-31 00:22:53.664223+00:00
		2023-10-31 00:22:54.684076+00:00
		2023-10-31 00:22:55.688829+00:00
		2023-10-31 00:22:56.700955+00:00
		2023-10-31 00:22:57.707923+00:00
		2023-10-31 00:22:58.713784+00:00
		2023-10-31 00:22:59.721037+00:00
		2023-10-31 00:23:00.723940+00:00
		2023-10-31 00:23:01.735039+00:00
		2023-10-31 00:23:02.749432+00:00
		2023-10-31 00:23:03.760042+00:00
		2023-10-31 00:23:04.770423+00:00

Exercise 2:	Destination IP -	93.184.216.34	
	Timestamps	HTTP -	2023-10-31 01:54:08.811061+00:00
			2023-10-31 01:54:08.873931+00:00
			2023-10-31 01:54:09.950735+00:00
			2023-10-31 01:54:10.122548+00:00
			2023-10-31 01:54:10.575292+00:00
			2023-10-31 01:54:18.826166+00:00
			2023-10-31 01:54:18.888188+00:00
			2023-10-31 01:54:19.964717+00:00
			2023-10-31 01:54:20.211863+00:00
			2023-10-31 01:54:20.584317+00:00
			2023-10-31 01:54:28.840190+00:00
			2023-10-31 01:54:28.901002+00:00
			2023-10-31 01:54:29.989211+00:00
			2023-10-31 01:54:30.224194+00:00
			2023-10-31 01:54:30.598076+00:00
		HTTPS -	2023-10-31 01:54:16.600849+00:00
			2023-10-31 01:54:18.682255+00:00
			2023-10-31 01:54:19.615851+00:00
			2023-10-31 01:54:19.631789+00:00
			2023-10-31 01:54:19.632213+00:00
			2023-10-31 01:54:19.639265+00:00
			2023-10-31 01:54:22.855451+00:00
			2023-10-31 01:54:22.877755+00:00
			2023-10-31 01:54:22.878381+00:00
			2023-10-31 01:54:22.891476+00:00
			2023-10-31 01:54:27.629060+00:00

Exercise 3:	Destination IP -	146.190.62.39	
	Timestamps	HTTP -	2023-10-31 02:24:36.709651+00:00
			2023-10-31 02:24:37.575787+00:00
			2023-10-31 02:24:46.716423+00:00
			2023-10-31 02:24:47.585385+00:00
		HTTPS -	2023-10-31 02:24:48.683834+00:00

Exercise 4:	Destination IP -	209.51.188.20
	Timestamps -	2023-10-31 02:29:04.324573+00:00

Exercise 5:	Destination IP -	205.166.94.9
	Timestamps -	2023-10-31 02:48:53.721845+00:00
		2023-10-31 02:48:54.052159+00:00
		2023-10-31 02:48:54.111013+00:00
		2023-10-31 02:48:58.440709+00:00
		2023-10-31 02:49:03.777652+00:00
		2023-10-31 02:49:03.952956+00:00
		2023-10-31 02:49:07.110722+00:00

4. For activities 2 and 3, can you tell which browser was used for these activities from the captured packets?

   There was no `User-Agent:` header in our header report in the script and in the Wireshark capture, so we were unable to find which browser was used.

3 Justifications and Assumptions

During the course of analyzing packets for 1A, we noticed that many TCP and TLS (specifically v1.2) packets were registered to either port 80 or port 443 for the source or destination machine. After a bit of querying online, we realized that these were HTTP/HTTPS packets on the application layer, but they were encrypted on the transport layer; namely by `TLSv1.2`. We decided to distinguish HTTP and HTTPS packets by registered `port 80` and `port 443` respectively, rather than what is conveyed as the operating Protocol in Wireshark, since much of live HTTP traffic is encrypted in the modern age. We believe this is a fair justification.

Furthermore, the activities suggest that we limit the traffic as much as we are able, but the recording machine experienced a lot of extraneous HTTP/HTTPS traffic, regardless of attempts to eliminate potential sources of such traffic. Web Browser extensions were removed, and a single tab was populated in the Firefox client. Because the questions do not indicate if the protocol enumeration and IP printout should be for the activity's server alone, as opposed to the entire capture we received while transmitting to the activity's server, we decided to include all application-layer protocols and IP's printouts for Questions 1, 2 and 3.

If a network analyst wished to acquire the subset of these packets which are retrievals or requests to the activity server, they could enforce an additional condition to only count HTTP/HTTPS protocols (and other relevant protocols) if the current source or destination IP of the current packet (depending on if it is response or request) corresponds to the activity server IP. We know the IP's for each activity, and it would be relatively trivial to implement them:

1. **https://google.com**: *142.250.189.206*
2. **https://example.com**: *93.184.216.34*
3. **https://httpforever.com**: *146.190.62.39*
4. **ftp.gnu.org**: *209.51.188.20*
5. **tty.sdf.org**: *205.166.94.4*

Keeping all of this in mind, we feel that this sufficiently demonstrates our knowledge of 1A.